TREND 9

Security by network

Aligning business and government interests for national security

Beth McGrath, Darren Hawco, Elizabeth Mardell, Adam Routh, and Akash Keyal

Introduction

On May 13, 1972, the newly christened *USS Nimitz* slid down Slipway 11 of Newport News Shipbuilding and Dry Dock Co., launching not just one ship but the largest class of warships ever built. Indeed, the *Nimitz*, at more than 1,000 feet long, was more: an advertisement for and indicator of American dominance in the entire scope of national security. The US government was the world's largest player in technology and innovation; lawmakers in Washington, D.C., could set industry agendas through purchases, grants, and regulations.

Decades later, the global security environment has shifted. The *Nimitz* class of warships would remain the world's largest for the next four decades, but they no longer served as the same metaphor for supreme federal power. Globally, commercial R&D spending eclipsed government levels, and democratizing technology meant that industrial decisions would now be driven by a host of different international public and private participants, each with differing agendas and incentives. When it comes to national security today, government is less an aircraft carrier than one ship—albeit a large ship—among many, with routes intersecting and crisscrossed with destinations varied.

Russia's invasion of Ukraine has highlighted this trend toward a more disaggregated, interest-driven world, with a wide range of public- and private-sector organizations making independent decisions, each with an impact on military and security outcomes.

Shortly after Russia's invasion of Ukraine, companies began to pull out of the Russian market, motivated not by any central security decision, such as a nation's imposition of sanctions, but by the diverse pull of shareholders and customers overwhelmingly opposed to Russia's actions and the business risk they believe resulted from Moscow's choices. The trend of disaggregated action continued as the conflict evolved. For example, when attacks threatened Ukrainian communications infrastructure, Ukraine's deputy prime minister tweeted an appeal to SpaceX, which moved quickly to provide Starlink internet service and terminals. The satellite-based technology's ubiquity and jamming resistance helped Ukraine, in the words of an adviser to President Zelenskyy, "survive the most critical moments of war." But the nation's appeal to and reliance on the actions of a private company—one based thousands of miles away, no less—to bolster its national security put Ukraine in an awkward position where it had to consider the interests of a private sector actor to preserve a critical wartime capability.

As governments around the world grapple with this trend, it is increasingly clear more collaboration with public and private participants is necessary to protect national security. Indeed, leaders are beginning to evolve new approaches and new tools to shape commercial partners' incentives and protect public security.

Walls coming down

- Traditional distinctions **between purely commercial and national security issues** are becoming increasingly fuzzy with corporate actions to pull out of countries, relocate manufacturing plants, or provide/deny service having significant national implications.
- Renewed **strategic competition between major powers is driving new collaboration between other nations** on issues beyond security as they find their interests currently aligned.
- Global, interdependent supply chains also increase the shared **risk for both government and businesses** as conflicts, or other disruptions, can cause whole industries to grind to a halt.

By the numbers: Security by network

Independent commercial decisions have an impact on security outcomes

1,000+

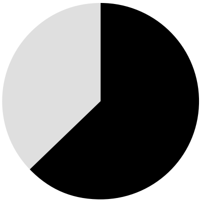
companies have curtailed operations in Russia since its invasion of Ukraine.

Increasingly blurred lines between good and bad actors in cybersecurity

● ● ● ●

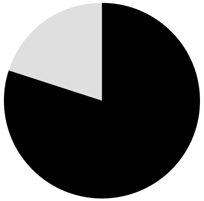
Researchers assess that at least four of the most advanced cyberthreat groups in the world are freelancers who work for both nation-states and criminal interests.

Consolidation of commercial supply chains can create national security vulnerabilities



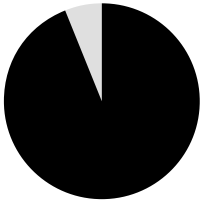
63%
Global market share in assembly, testing, and packaging of semiconductors

Taiwan
China
South Korea
Japan



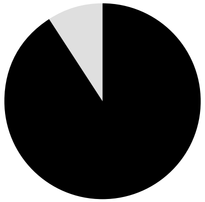
80%
Global market share in photovoltaic cell manufacturing

China



94%
Global market share in rare earth permanent magnet production

China



91%
Global market share in rare earth metal or alloy production

China

Sources: CELI, “Over 1,000 companies have curtailed operations in Russia—but some remain,” February 8, 2023; Mandiant, “Advanced persistent threats (APTs),” accessed February 9, 2023; Saif M. Khan, Alexander Mann, and Dahlia Peterson, *The semiconductor supply chain: Assessing national competitiveness*, CSET, January 2021; US Department of Energy, *Solar Photovoltaics*, February 24, 2022; Vasileios Rizos, Edoardo Righetti, and Amin Kassab, "Developing a supply chain for recycled rare earth permanent magnets in the EU," CEPS, December 2022.

Trend in action

The breaking down of these walls is creating perceptible shifts in how national security is achieved.

Shift from central control to disaggregated action

Once centrally controlled, security is now increasingly driven by the actions of disaggregated players. For example, military supplies traditionally flowed to foreign countries through a closely regulated sales process tightly controlled by ministries or departments of defense. But the increasing dual-use applicability of consumer technologies to military tasks means that suppliers increasingly have the opportunity to sell directly to militaries around the world. Defense ministries already purchase consumer-grade drones, hacking software, and more—SpaceX developed its Starlink internet system for consumers, not for Ukrainian national security.

And if companies are free to **do** business with countries, they can choose **not to** do business as well. Traditional government tools such as economic sanctions or military blockades have long controlled the process of limiting a country's markets to certain buyers, but corporations pulling out of Russia showed that the same effect could be achieved by individual companies electing—based on their own commercial interests—to no longer do business there. While the Russia pullouts happened to align with Western nations' security goals, they raise the troubling issue of whether a government could influence, much less control, such actions if commercial incentives and national security interests pulled in opposite directions.

The intelligence space is confronting rising tensions between security needs and other potentially competing incentives. The proliferation of commercial satellite imagery, online data, and, especially, social media has given amateur analysts the tools to track even sensitive military radar systems in real-time while sitting at their kitchen tables. While internet detectives had used these tools to do everything from tracking warship deployments in the Syrian conflict to identifying those responsible for downing Malaysian Air flight 17, the Ukraine conflict focused fresh attention on the trend. In advance of Russia's invasion, online communities were able to track and share details of Russian troop buildup and accurately predict the invasion's movements. Once the invasion began, communities used social media posts and facial recognition to identify individual Russian service members serving in Ukraine, particular munitions used, and even members of a clandestine Russian military unit programming missile flight paths.

Again, in all of these cases, the actions of these online sleuths aligned with key Western security goals. But there's no guarantee that future independent initiatives will share those objectives.

The clash of familiar roles and shifting interests

The proliferation of players now acting in the security space means that government must adjust traditional roles to work within a more diverse ecosystem, often only able to exert influence—not control. In place of fixed rules set by a department of state or ministry of defense, each participant is often guided by their own unique, ever-shifting set of incentives: how they can make money, what sales and activities align with stated organizational values or brand, how certain contracts might conflict with others, and so on. The way a government agency is currently organized or equipped may not be suited to meet changing private-sector incentives.

Nowhere might this struggle between government roles and industry incentives be more visible than in cyberspace, where lines between sanctioned and freelance, legitimate and rogue, often blur. In April 2022, a Russian hacker group launched a ransomware attack on the government of Costa Rica, crippling the nation's electric grid. As with previous cyberattacks on Brazil and Argentina, Costa Rica found itself in discussions and negotiations with other governments, private companies, and hackers to bring the issue to resolution.

The conflict in Ukraine sounded a clarion call for online freelancers on all sides, guided largely by their own sense of right and wrong: Russia-backed hackers aimed to take down Ukrainian government websites; Western hackers targeted Russian sites and even Russia-backed hackers themselves. And this activity often occurred without state sanction and, thus, outside of any internationally agreed-upon principles of conduct. This type of behavior—which will likely become more common—not only complicates attribution and response by other nations but can make these activities difficult for even an aligned state to control. What do you do if a hacker invokes your nation's name in taking down a hospital, whether in an allied or enemy country? Are you legally responsible? Can an adversary legitimately encourage its own freelance hackers to respond?

Finding mechanisms to coordinate these disaggregated, interest-driven actions is key to solving or at least mitigating these difficult possibilities.

This shift challenges traditional tools

For government leaders looking to steer behaviors through a new set of incentives, the challenge is exacerbated by the ineffectiveness of many traditional tools. National security is increasingly tangled with economic and other considerations.

Take semiconductors, for instance. A critical component of electronic devices, from personal vehicles to fighter jets, semiconductor availability is vital to a country's economic and national security. But their production is highly concentrated, with companies in Taiwan, the United States, China, and South Korea owning 84% of the global market share in assembly, testing, and packaging. Furthermore, just two regions—Taiwan and South Korea—manufacture nearly all advanced chips. This concentration creates supply chain chokepoints and vulnerabilities, which could leave entire industries and countries without access to semiconductors during heightened geopolitical tensions or other trade disruptions.

As the COVID-19 pandemic and the Russian invasion of Ukraine disrupted a range of global supply chains, some governments moved to bolster or jumpstart domestic semiconductor industries: The European Union recently announced a €43 billion EU Chips Act with the aim of making the region self-sufficient in semiconductors, while the US government's CHIPS Act laid out plans for more than US$52 billion in federal funding. Yet some governments—especially those without the means to stand up a new high-tech industry—may have little choice but to deal with an uncomfortably tenuous supply chain.

The promise of making national security more, well, secure—aligning the interconnected challenges of semiconductors, cybersecurity, and open-source intelligence, among other areas—demands tools more fine-grained than the blunt instruments of export controls and similar regulations. Agencies need agile tools that can inform and align private-sector interests and guide decisions without costly consequences for government or industry.

Efforts to shore up vulnerabilities have thus far focused on encouraging closer collaboration around shared interests. For example, the FY2023 US National Defense Authorization Act requires key government agencies to study how to build a more collaborative cyber information environment. The European Union has also doubled down on collaboration through Horizon Europe, a research and innovation program with particular emphasis on pressing transnational or regional issues, such as climate change and support to Ukraine. The program pays special attention to open-science policies and new approaches to partnerships with industry. It's likely that governments and agencies will further expand such initiatives as national security ecosystems continue to sprawl.

Battling botnets

Governments, often through law enforcement agencies, have traditionally taken the lead in investigating and preventing crime. But in the cyber domain, tech giants such as Google, which see a huge chunk of global internet traffic pass through their systems daily, are increasingly incentivized to take down wrongdoers.

Governments had long tracked the Glupteba botnet. Spread by tricking users into downloading malware via third-party "free download" sites; the malware would then steal user credentials and data, secretly mine cryptocurrencies on infected hosts, and use infected machines and routers to channel other people's internet traffic. Glupteba posed a real and growing threat to not only victims' finances but entire systems, both private and public.

Google took the initiative to study the extent of the problem and found that Glupteba had infected around one million devices worldwide and that hackers were using Google's own services to distribute the malware. Google moved to shut it down. The company terminated around 63 million Google Docs, more than 1,000 Google accounts, and over 900 Google Cloud projects that hackers were using to distribute Glupteba. Google also worked with internet infrastructure companies worldwide to disrupt the botnet's command-and-control infrastructure, preventing infected devices from receiving new commands from their controllers. And Google successfully sued two Russia-based hackers it alleged were behind Glupteba's operations. The effort suggests how broad cybersecurity moves may be increasingly public-private partnerships.

Moving forward

A more disaggregated and interest-driven world means that government agencies and ministries cannot go it alone even when it comes to national security, a role topping any list of government responsibilities. Increasingly, governments must collaborate with a broad ecosystem that includes a wide variety of players—often quickly, with crises and events still developing—to advance national security outcomes. If that collaboration is well-managed, new and more effective security capabilities may emerge. Recommendations to establish and manage that collaboration include:

- **Be receptive to shifting interests and adjust plans accordingly.** As is evident from the private-sector pullout in Russia, companies' interests can change rapidly. Government and business leaders should carefully assess the significance of changing interests to identify where opportunities for collaboration exist and where they may arise, communicating to discuss potentially aligned agendas. For government agencies and ministries, this may mean challenging entrenched organizational culture and assumptions that may blind people to the realities of a changing world. For business leaders, this may mean not waiting until government requests and/or requires action but, rather, being proactive in recognition of shifting security imperatives as well as business interests.

- **Identify bridgebuilders who can span both worlds.** Whether in industry, academia, or government, sectors often speak different languages. Finding leaders who understand the nuances of various interests and can translate is often a first step to establishing the trust and communication necessary to work together on tough security issues. Recognized bridgebuilders need to be empathetic of partners and their positions and be incentivized to grow strong relationships around shared—or at least not opposing—interests.

- **Create platforms for collaboration.** Once initial trust has been established, government and the private sector need forums where they can share information and work out the details of the collaboration. These forums should be outcome-oriented, flexible in design, quick to stand up, and easy to dissolve as interests shift. The internet governance community offers this through various technical and policy working groups and task forces.

- **Take an iterative approach.** Finally, wherever conflicting interests are concerned, progress will not be instantaneous or assured—especially when the stakes are so high. But the consequences of conflicting government and private-sector interests are likely to impair security equally. Where collaboration proves difficult, remain agile in changing people, processes, and techniques to allow new ideas, tools, and practices to break barriers. Sustained dialogue over time will create opportunities for increased alignment and collaboration.

My take

David Perry
PhD, president and senior analyst,
Canadian Global Affairs Institute

Aligning national and commercial interests requires new forms of knowledge-sharing and collaboration

The last few years have brought into sharp focus the tension between industry and government interests and the need to work together in response to a seemingly ever-shifting national security landscape. In Canada, we've seen the COVID-19 pandemic, supply chain issues, and Russia's invasion of Ukraine stress government and industry's capacity to respond to unexpected national security threats. Whether the goal is to quickly procure personal protective equipment to save lives during the pandemic or provide timely critical aid to Ukraine, government and industry tend to understand what a good solution looks like, but struggle to identify and align interests to realize it, at least at first.

This tends to stem from weak linkages between government and industry, leading to poor knowledge-sharing. Indeed, assumptions often underwrite too much of government and industry's relationship: what industry may assume the government needs or government's assumptions about the risks or vulnerabilities that might be influencing industry interests. This problem makes it difficult to identify shared interests, synchronize resources, and identify courses of action across the national security enterprise.

Strengthening industry and government linkages to align interests requires new forms of knowledge-sharing and collaboration. Improving knowledge-sharing requires better communication between government and industry, with particular focus on avoiding assumptions about what the other may know or need. A strong dialogue should include a process for quickly understanding what resources or solutions each can bring to a problem set and what each needs to offer additional solutions. Improving collaboration should include joint efforts to forecast national security needs, enabling government and industry to identify cross-sector solutions and any challenges that may impede a desired response. Improved collaboration should also include mechanisms to act before a forecast risk becomes real.

At the Canadian Global Affairs Institute, we've been working to prompt conversations on improving industry and government linkages. Our recent conference assessing defence procurement challenges, including rebuilding the industrial base and overcoming labor shortages, is one such example. We understand that as the national security environment changes, the relationship between industry and government will also change, and that they must make these changes together.

Endnotes

1. U.S. Carriers, "USS NIMITZ CVN 68," accessed December 15, 2022.
2. Naval Technology, "Nimitz Class Aircraft Carrier," January 6, 2020.
3. Shamseer Mambra, "USS Nimitz: One of the biggest war ships in the world," *Marine Insight*, August 7, 2011; Naval Technology, "Nimitz class aircraft carriers," January 6, 2020.
4. Rebecca Mandt, Kushal Seetharam, and Chung Hon Michael Cheng, *Federal R&D funding: The bedrock of national innovation, MIT Science Policy Review 1*, August 20, 2020, pp. 44-54.
5. Irina Ivanova and Kate Gibson, "These are the companies that have pulled out of Russia since its invasion of Ukraine," *CBS News*, March 11, 2022; *New York Times*, "Companies are getting out of Russia, sometimes at a cost," October 14, 2022.
6. Nicolas Boyon, "Global public opinion about the war in Ukraine," Ipsos, April 19, 2022.
7. Jeff Foust, "SpaceX worked for weeks to begin Starlink service in Ukraine," *SpaceNews*, March 8, 2022; Minda Zetlin, "Here's the untold story of how a single tweet to Elon Musk changed history," Inc.com, March 26, 2022.
8. Isabelle Khurshudyan et al., "Musk threatens to stop funding Starlink internet Ukraine relies on in war," *Washington Post*, October 14, 2022.
9. Matt Binder, "Providing Starlink to Ukraine was Elon Musk's biggest PR victory. Now he doesn't even want to do that," *Mashable*, October 14, 2022.
10. Nicholas Gordon, "Chinese drone maker DJI has suspended sales in both Ukraine and Russia, where its consumer tech was deployed in war," *Fortune*, April 27, 2022; Mark Mazzetti, Ronen Bergman, and Matina Stevis-Gridneff, "How the global spyware industry spiraled out of control," *New York Times*, December 10, 2022.
11. Belinda Luscombe, "Hundreds of CEOs came out against Russia. Their involvement could change war forever," *Time*, March 11, 2022.
12. Ollie Ballinger, "Radar Interference Tracker: A new open source tool to locate active military radar systems," Bellingcat, February 11, 2022.
13. Karl Vick, "Bellingcat's Eliot Higgins explains why Ukraine is winning the information war," *Time*, March 9, 2022.
14. Thomas Eydoux, "Meet the anonymous internet investigators tracking Russian movements on the Ukrainian border," *The Observers*, February 10, 2022.
15. Tom Simonite, "Online sleuths are using face recognition to ID Russian soldiers," Wired, March 10, 2022.
16. Janosch Deeg, "How Bellingcat investigators verified the brutal use of cluster munitions in Ukraine," *Scientific American*, March 18, 2022.
17. Christo Grozev, "The remote control killers behind Russia's cruise missile strikes on Ukraine," Bellingcat, October 24, 2022.
18. Paul Brian, "Ransomware hackers declare total war on Costa Rica," *National Interest*, May 22, 2022.
19. Carmela Chirinos, "Russian hackers started a vigilante cyber militia to take down Ukraine's websites and steal data," *Fortune*, February 25, 2022; *Reuters*, "Russian ministry website appears hacked; RIA reports users data protected," June 5, 2022.
20. Ibid.
21. Simon Handler and Liv Rowley, "The 5x5—cybercrime and national security," Atlantic Council, June 29, 2022; Lucas Ropek, "Are hackers targeting critical infrastructure more often?", *Government Technology*, March 3, 2020.
22. Saif M. Khan, Alexander Mann, and Dahlia Peterson, "The Semiconductor Supply Chain: Assessing National Competitivenessk," Center for Security and Emerging Technology, January 2021.
23. Deloitte Center for Government Insights, Boosting resilience: Working with like-minded partners to orchestrate critical supply chains, Deloitte, 2022.
24. Melanie Rojas et al., *Reshoring and "friendshoring" supply chains*, Deloitte Insights, March 24, 2022.
25. European Commission, "European Chips Act—questions and answers," February 8, 2022.
26. Nihal Krishan, "NDAA requires intelligence agencies to study creation of cyber collaboration program," *FedScoop*, December 8, 2022.
27. European Commission, "Horizon Europe," accessed December 20, 2022.

Endnotes

28. Shane Huntley and Lucy Nagy, “Disrupting the Glupteba operation,” Google Blog, December 07, 2021.

29. Gerrit De Vynck, “Google disrupted a massive botnet that hackers used to steal information and mine cryptocurrency,” *Washington Post*, December 7, 2021.

30. oyal Hansen and Halimah DeLaine Prado, “A ruling in our legal case against the Glupteba botnet,” Google, November 18, 2022.

31. William D. Eggers and Donald Kettl, B*ridgebuilders: How Government Can Transcend Boundaries to Solve Big Problems* (Cambridge MA: Harvard Business Review Press), 2023.

Acknowledgments

The authors thank **Joe Mariani** for his insights and thoughtful feedback on the draft. They would also like to thank **Meenakshi Venkateswaran** for helping design the infographics of the article.

About the authors

Beth McGrath

bmcgrath@deloitte.com

Beth McGrath is Deloitte's global leader for government and public services. In her role, she is committed to strengthening synergies across global industries and government and public services with a focus on client mission needs and solutions. McGrath has broad, multidisciplinary, strategic, and operational management experience acquired from 25+ years of successful performance in the United States government sector.

Darren Hawco

dhawco@deloitte.ca

Darren Hawco is an executive advisor in the Monitor Deloitte strategy practice. He is a retired vice admiral from the Royal Canadian Navy and an executive with extensive public, military, and allied services experience. Hawco is particularly skilled in intelligence, operational, and tactical planning, as well as capability design and crisis and operations management. Hawco holds a master of defence policy and a master of public administration focused in defense policy and public administration from Royal Military College of Canada.

Elizabeth Mardell

emardell@deloitte.co.nz

Elizabeth Mardell leads Deloitte's Defense team in New Zealand. Her work focuses on decision-making for infrastructure-intensive entities, particularly in the public sector. She is passionate about investigating investment opportunities, solving problems, and connecting with project teams. Mardell's experience spans areas such as defense, transport, justice, education, and culture and heritage.

Adam Routh

adrouth@deloitte.com

Adam Routh is a manager with Deloitte's Center for Government Insights and a PhD student in the defense studies department at King's College London. His research areas include space policy, the future of defense, and great power competition. Routh's research has addressed US national space policy, space governance, the challenges and requirements of the future military force, and emerging technologies. His analysis has been featured on the nightly news and the John Batchelor Show and published in *National Review, The Hill, The National Interest, Space News, The Space Review, Real Clear Defense,* and *Defense News*, among other outlets.

Akash Keyal

akkeyal@deloitte.com

Akash Keyal is a research specialist within the Deloitte Center for Government Insights. He specializes on issues related to defense, security, and justice (DS&J), and climate change.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

Beth McGrath

Managing Director | Deloitte Consulting LLP
+1 571 882 8455 | **bmcgrath@deloitte.com**

Beth McGrath is Deloitte's global leader for Government and Public Services. In her role, she is committed to strengthening synergies across global Industries and government and public Services with a focus on client mission needs and solutions.

The Deloitte Center for Government Insights

William D. Eggers

Executive director | Deloitte Center for Government Insights | Deloitte Services LP
+1 571 882 6585 | **weggers@deloitte.com**

William D. Eggers is the executive director of Deloitte's Center for Government Insights, where he is responsible for the firm's public sector thought leadership.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte offers national security consulting and advisory services to clients across the Department of Defense, the Department of Homeland Security, the Department of Justice, and the intelligence community. From cyber and logistics to data visualization and mission analytics, personnel, and finance, we bring insights from our client experience and research to drive bold and lasting results in the national security and intelligence sector. Our people, ideas, technology, and outcomes are all designed for impact. To learn more, visit Deloitte.com.

Deloitte.
Insights

Sign up for Deloitte Insights updates at **www.deloitte.com/insights**

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Ramani Moses, Abrar Khan, Arpan Kumar Saha, Emma Downey, Aparna Prusty, and Shambhavi Shah
Creative: Natalie Pfaff, Jaime Austin, Meena Sonar, Rahul B, and Govindh Raj
Deployment: Kelly Cherry, Maria Martin Cirujano, and Nikita Garia
Cover artwork: Natalie Pfaff

About Deloitte Insights
Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.
Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication
This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.